UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/809,030	03/16/2001	Yuval Ben-Itzhak	032272.0003	5590

21967 7590 10/01/2004

HUNTON & WILLIAMS LLP
INTELLECTUAL PROPERTY DEPARTMENT
1900 K STREET, N.W.
SUITE 1200
WASHINGTON, DC 20006-1109

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/809,030	BEN-ITZHAK, YUVAL	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-54 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-4,7,9-12,15,16,18-22,25-33,36-43 and 46-54 is/are rejected.

7)☒ Claim(s) 5,6,8,13,14,17,23,24,34,35,44 and 45 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 09202004.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-4, 7 are rejected under 35 U.S.C. 102(b) as being anticipated by BRP publications.

3. As per claim 1, BRP publications teaches a method for protecting an application from executing an illegal or harmful operation request received from a distrusted environment, BRP teaches this, because BRP teaches that Appshield, protects the integrity of an e-commerce application by making it nearly impossible for hackers to use traditional security loopholes, either in the application code or web servers(see lines 27-29). Also, BRP publications teaches determining whether said operation request is illegal or harmful to an environment of said application, and preventing an application from executing an illegal or harmful operation request, because Appshield rejects unexpected, illegal inputs, generating an error page for the user and notifying the management(see lines 30-33).

4. As per claim 2, BRP publications discloses wherein the illegal and harmful operation request causes damage, because Appshield is designed to protect applications from illegal operations(see lines 27-31). BRP publications teaches that these illegal operations are performed by hackers(see lines 27-31). Also, BRP publications teaches that hackers threaten the effectiveness of Internet transactions(see lines 1-5). BRP teaches that a hacker could

fraudulently change the prices on a particular item online and purchase it at that price, he could tape into secret medical records; or access private passwords to log on to information on a site(see lines 6-11). The Examiner asserts that these are all illegal and harmful operations that cause damage.

5. As per claim 3, BRP publications teaches wherein said illegal and harmful operation request is database manipulation, because BRP teaches that an hacker could access private passwords to log on to a particular site(see lines 7-9).

6. As per claim 4, BRP publications teaches wherein said step of preventing includes the step of rejecting said illegal or harmful operation request, Appshield prevents illegal or harmful operation request, by rejecting them, because BRP publications teaches Appshield rejects unexpected, illegal inputs(see lines 30-32).

7. As per claim 7, BRP publications teaches wherein said step of determining includes the step of checking said operation request for an existence of an embedded command causing database manipulation(see lines 6-11, 22-26).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 9-12, 15-16, 18-22, 25-33, 36-43, 46-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over BRP publications in view of Reshef et al(6,584, 569).

10. As per claim 9, BRP publications does not teach parsing said operation request into one or more expressions; building a state-automate; inspecting said one or more expressions for improper syntax and characters not defined in a first alphabet; and applying said state-automate to said operation request. However, Reshef et al. discloses parsing said operation request into one or more expressions; building a state-automate; inspecting said one or more expressions for improper syntax and characters not defined in a first alphabet; and applying said state-automate to said operation request(see col. 6, lines 41-67, col. 8, lines 61-67, col. 9, lines 1-3). It would have been obvious to one of ordinary skill in the art at the time of the invention to include the parser of Reshef et al. with BRP publications, the motivation to include the parser is, the parsing engine, extracts any path parameters, and is parsed to identify other application interface elements such as data parameters (see col. 6, lines 41-49 of Reshef). Thus, parsing of Reshef identifies any input or hidden fields such as those associated with HTML forms(see col. 6, lines 50-53 of Reshef).

14. As per claim 10, BRP publications does not include encoded characters. However, Reshef et al. discloses encoded characters (see col. 6, lines 41-49). It would have been obvious to include encoded character of Reshef in BRP publications, the motivation is that web applications interface with external clients sing a multitude of parameters, and these parameters have a number of attributes, data type, length, visibility, and value(see col. 7, lines 36-50 of Reshef).

15. As per claim 11, BRP publications does teaches the following limitations; however, Reshef discloses wherein said step of determining comprises the steps of: comparing said

operation request against stored known vulnerability patterns to determine a match; and blocking said operation request if said match is found(see col. 4, lines 9-32, col. 8, lines 36-51). It would be obvious to one of ordinary skill in the art at the time of the invention to include comparing the operation request against stored known vulnerability patterns and blocking, the motivation is that application level vulnerabilities have traditionally been discovered and reviewed by developers; who have to review the application line-by-line and understand the code to try to imagine or anticipate potential security loopholes(see col. 1, lines 62-67, col. 2, lines 1-13 of Reshef). Developers lack the expertise and knowledge to evaluate security flaws, and applications are constantly changing. Therefore, Reshef discloses a scanner that detects security vulnerabilities in applications, and stores the vulnerabilities and updates(see col. 4, lines 9-32).

16. As per claim 12, BRP publications does not teach the following limitations; however, Reshef discloses the step of: updating said stored vulnerability patterns with newly found vulnerability patterns(see col. 8, lines 36-46). It would be obvious to one of ordinary skill in the art at the time of the invention to include updating the stored vulnerability patterns with newly found vulnerability patterns of Reshef with BRP publications, the motivation is that application level vulnerabilities have traditionally been discovered and reviewed by developers; who have to review the application line-by-line and understand the code to try to imagine or anticipate potential security loopholes(see col. 1, lines 62-67, col. 2, lines 1-13 of Reshef). Developers lack the expertise and knowledge to evaluate security flaws, and applications are constantly changing. Therefore, Reshef discloses a scanner that detects security vulnerabilities in applications, and stores the vulnerabilities and updates(see col. 4, lines 9-32 Reshef).

17. As per claim 15, BRP publications does not teach the following limitations; however, Reshef discloses dividing said operation request into four zones(see col. 8, lines 1-7); comparing each of said four zones against stored known vulnerability patterns to determine a match; and blocking said operation request if said match is found(see col. 6, lines 1-12, col. 9, lines 32-53). It would have been obvious to one of ordinary skill in the art at the time of the invention to include the four zones of Reshef with BRP publications, the motivation is that these four zones of Reshef are used to detect hacking of applications(see col. 3, lines 60-67, col. 4, lines 1-8, col. 7, lines 51-67).

18. As per claim 16, BRP publications does not teach the following limitations; however, Reshef discloses wherein said four zones represent a URI, query string, header, and body associated with said operation request(see col. 6, lines 1-12, col. 8, lines 1-7, col. 9, lines 32-53). It would have been obvious to one of ordinary skill in the art at the time of the invention to include the four zones of Reshef with BRP publications, the motivation is that these four zones of Reshef are used to detect hacking of applications(see col. 3, lines 60-67, col. 4, lines 1-8, col. 7, lines 51-67).

19. As per claim 18, BRP publications does not teach the following limitations; however, Reshef discloses determining a first set of internal URLs and parameters values contained in said reply(see col. 5, lines 44-50); receiving a second operation request in response to said reply(see col. 6, lines 1-12); comparing a second set of internal URLs and parameters values contained in said second operation request with said first set to determine if said sets correspond; and rejecting said second operation request if said sets do not correspond(col. 6, lines 26-40, col. 8, lines 1-5, 21-34, col. 9, lines 48-53). It would have been obvious to one of ordinary skill in the

art at the time of the invention to include a set of internal URLs and parameter values contained in the reply, the motivation to include an internal Url, and comparing the internal Url, is that online theft, can be prevented by examining the Url(see col. 7, lines 51-67 of Reshef et al.).

20. As per claim 19, BRP publications does not teach the following limitations; however, Reshef discloses identifying a single client to interact with said application (see col. 3, lines 44-49); determining a first set of parameter names and values in said reply(see col. 3, lines 49-54); receiving a second operation request from said client in response to said reply; determining a second set of parameter names and values in said second operation request; and forwarding said second request to said application only if said first set matches said second set(see col. 3, lines 60-67, col. 4, lines 1-8). It would have been obvious to one of ordinary skill in the art at the time of the invention to include a parameter name and values in the reply, the motivation is that a hacker can alter the numeric input field, and freeze the application, thus the scanner looks and the list of vulnerabilities (see col. 3, lines 60-67, col. 4, lines 1-8 of Reshef).

22. As per claim 20, BRP publications does not teach designating an application path of the application restricted; determining a destination of the operation request; and blocking the operation request if the destination is equal to designated path, Reshef discloses designating an application path of the application restricted; determining a destination of the operation request; and blocking the operation request if the destination is equal to designated path(see col. 8, lines 61-67, col. 9, lines 1-3, 31-53). It would have been obvious to one of ordinary skill in the art at the time of the invention to include the application path of the application restricted with BRP publications, the motivation is that the detection phase searches for application path parameters in order to check for a vulnerability (see col. 3, lines 60-67).

23. As per claim 21, BRP publications does not teach the following limitations; however, Reshef discloses compiling a list of acceptable operation requests; and comparing said operation request to said list of acceptable operation requests(see col. 4, lines 15-19, col. 8, lines 36-51). It would have been obvious to one of ordinary skill in the art at the time of the invention to include a compiling list of acceptable operations request from Reshef with BRP publications, the motivation is that the scanner of Reshef includes predefined rules which are used to create http requests based on vulnerabilities with platforms that can be employed at the web application(see col. 4, lines 8-19 of Reshef).

24. As per claim 22, BRP publications is silent on the following limitations; however, Reshef discloses determining a parameter value contained within said operation request(see col. 3, lines 44-54); and applying a pre-defined rule to said parameter based on said parameter type, wherein said pre-defined rule defines one or more acceptable parameter values(see col. 3, lines 60-67, col. 4, lines 1-19). It would have been obvious to one of ordinary skill in the art at the time of the invention to include determining a parameter value contained within the operation request of Reshef with BRP publications, the motivation is that the scanner can dynamically traverse the web application to examine the attributes of the path and data parameters for hackers modifying input fields(see col. 3, lines 44-66).

25. As per claim 25, BRP publications does not teach the following limitations; however, Reshef discloses storing said plurality of operation requests into a virtual directory(see col. 8, lines 13-20); building a dynamic range of entered values for each parameter in said plurality of operation requests(see col. 8, lines 61-67, col. 9, lines 1-3, col. 10, lines 1-20); computing an acceptable range of values for each parameter based on a statistical model applied to said

dynamic range of entered values for each value(see col. 10, lines 1-35, 56-60); receiving a subsequent operation request; identifying parameter values in said subsequent operation request; and determining if said parameter values in said subsequent operation request are within said acceptable range of values(see col. 8, lines 61-67, col. 9, lines 1-3). It would have been obvious to one of ordinary skill in the art at the time of the invention, to include adding parameter values in subsequent operation request to dynamic range, the motivation is that the mutated requests can be initiated during the attack stage to evaluate the real threat that the potential vulnerabilities pose(see col. 10, lines 40-48 of Reshef et al.).

26. As per claim 26, BRP publications does not teach including the steps of: adding said parameter values in subsequent operation request to dynamic range; adjusting said acceptable range of values for each parameter by applying said statistical model. However, Reshef et al. discloses adding said parameter values in subsequent operation request to dynamic range; adjusting said acceptable range of values for each parameter by applying said statistical model(see col. 9, lines 60-67, col. 10, lines 1-48). It would have been obvious to one of ordinary skill in the art at the time of the invention, to include adding parameter values in subsequent operation request to dynamic range, the motivation is that the mutated requests can be initiated during the attack stage to evaluate the real threat that the potential vulnerabilities pose(see col. 10, lines 40-48 of Reshef et al.).

27. As per claim 27, BRP publications does not teach the following limitations; however, Reshef et al. discloses a system for implement an application security layer between a trusted application and a distrusted computer environments including: means for receiving an operation request(see col. 3, lines 44-58)for said application; means for embedding said operation request

into a data format used by said trusted application(see col. 3, lines 60-67, col. 4, lines 1-8)an encoder for encoding said operation request according to an encoding scheme; and means for applying a pipe to each operation request, wherein the number and types of pipes applied to each operation request are based on said resolved destination node of each operation request(see col. 4, lines 1-30). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine BRP with Reshef, both teaches protecting an application from hackers, the motivation to protect application from hackers is that a hacker can alter a parameter in an http request, and freeze the application (see col. 4, lines 1-8).

28. As per claim 28, BRP publications teaches wherein the designated communications protocol is http(see lines 22-31).

29. As per claim 29, BRP publications inherently teaches wherein said encoding scheme is ASCII, because BRP publications teaches http application protocol(see lines 22-31), http uses ASCII.

30. As per claim 48, BRP publications teaches a system for implement an application layer security layer between a trusted application and a distrusted computer environments including means for receiving an operation request for the application (see lines 16-19); means for embedding the operation request into a data format used by the trusted application (see lines 30-33), and means for checking a contents of the operation requests to identify if the operation request is illegal or harmful to an environment of the application(see lines 27-29). BRP publications does not disclose illegal or harmful to an environment of the application that consists of uniform resource identifier. However, Reshef et al. discloses wherein the illegal or harmful request consists of uniform resource identifier (see col. 6, lines 1-12, 49-56). It would

have been obvious to one of ordinary skill in the art at the time of the invention to include the uniform resource identifier, the motivation is that online theft is one vulnerability that a hacker can change the purchase price by changing the value of the parameter in the http request, thus by checking a uniform resource identifier online theft can be prevented (see col. 7, lines 51-67).

31. As per claim 49, BRP publications teaches wherein said data format is selected from HTTP(see lines 22-31).

32. As per claim 50, BRP publications inherently discloses wherein said receiving means is a queued socket server, because BRP publications teaches that e-commerce applications are protected from hackers, e-commerce use socket server to protect data(see lines 22-29).

33. As per claim 54, BRP publications teaches means for providing a firewall, is inherent in BRP, because BRP teaches that Appshield teaches a policy recognition engine(see lines 22-24). Also, BRP publications teaches that Appshield recognizes the intended application security policy by analyzing each outbound hypertext markup language page, and enforces compliance with the policy for each incoming application(see lines 22-26).

34. As per claim 30, it is rejected under the same basis as claim 9. Further, the application of the pipe of Reshef is the scanner(see col. 44-53).

35. As per claim 31, it is rejected under the same basis as claim 10.

36. As per claim 32, it is rejected under the same basis as claim 11.

37. As per claim 33, it is rejected under the same basis as claim 12.

38. As per claim 36, it is rejected under the same basis as claim 15.

39. As per claim 37, it is rejected under the same basis as claim 16.

40. As per claim 38, it is rejected under the same basis as claim 17.

41. As per claim 39, it is rejected under the same basis as claim 18.

42. As per claim 40, it is rejected under the same basis as claim 19.

43. As per claim 41, it is rejected under the same basis as claim 20.

44. As per claim 42, it is rejected under the same basis as claim 21.

45. As per claim 43, it is rejected under the same basis as claim 22.

46. As per claim 46, it is rejected under the same basis as claim 25.

47. As per claim 47, it is rejected under the same basis as claim 26.

48. As per claim 51, limitations have already been addressed (see claim 27).

49. As per claim 52, it is rejected under the same basis as claim 49.

50. As per claim 53, it is rejected under the same basis as claim 29.

51. As per claims 5-6, 8, 17 are objected to, because base claims rejected. Claims 5-6, and 8 are objected to, because prior art nor non-patent literature disclose or teach, modifying the illegal or harmful operation into a legal or harmless operation, because the prior art discloses that when an illegal or harmful operation is detected it is analyzed and logged, does not disclose modifying the operation to a legal request.

52. As per claims 13-14, 34-35 are objected to, because base claims rejected. Claims are objected to because of computing a hash value for every consecutive specified number of character in the operation request, and comparing every has value to stored hash values. Prior art nor non-patent literature discloses computing hash values for a number of characters, the prior art discloses looking for parameters and checking for tampering of the application, not computing a hash value for the characters.

53. As per claims 23-24, 44-45 are objected to, because base claims rejected. Claims are objected to because of decrypting values in the cookie message header and modifying the operation request to reflect the decrypted values. Prior art fails to disclose these limitations. An example of prior art that does not disclose these is Reshef. Reshef discloses cookie values are checked to see if they have been manipulated. Non-patent literature teaches cookie poisoning, which a hacker can take on another's identity online. However, prior art fails to disclose the limitations above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

Jenise Jackson

September 21, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100